

AF
Ifw

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on October 5, 2006.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Examiner: Thomas M. Szymanski

Group Art
Unit: 2134

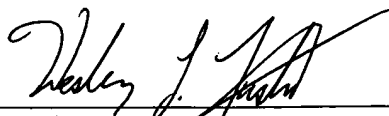
Page 1 of 2

Appl. No. 10/027,714

Appeal Brief Dated September 5, 2006

Reply to Notification of Non-Compliant Appeal Brief of September 18, 2006

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Wesley L. Austin', written over a horizontal line.

Wesley L. Austin

Reg. No. 42,273

Attorney for Appellant(s)

Date: October 5, 2006

Wesley L. Austin, Esq.

Trapware Corporation

1244 E. 1650 S.

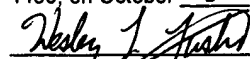
Bountiful, UT 84010

Telephone: (801) 296-0597

Appl. No. 10/027,714
Appeal Brief Dated September 5, 2006
Reply to Office Action of April 7, 2006

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on October 5, 2006.



Attorney for Applicant(s)

PATENT APPLICATION
Docket No. AUZ-002 P

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): David M. Austin et al.

Serial No.: 10/027,714

Filed: December 21, 2001

For: DETECTION OF OBSERVERS AND
COUNTERMEASURES AGAINST OBSERVERS

Examiner: Thomas M. Szymanski

Group Art
Unit: 2134

APPEAL BRIEF - CORRECTED

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

An Office Action dated April 7, 2006 rejected all pending claims (claims 1-21) in the present application. A timely Notice of Appeal was mailed on July 6, 2006 and was received by the United States Patent Office on July 10, 2006. Appellants' Appeal Brief is being filed herewith.

1. REAL PARTY IN INTEREST

The real party in interest is the assignee, Trapware Corporation.

2. RELATED APPEALS AND INTERFERENCES

An appeal had been filed in the parent patent application, Application No. 09/491,727. A Notice of Appeal was filed on June 6, 2005. In response to the Notice of Appeal and Appeal Brief, the finality of the last office action on App. No. 09/491,727 was withdrawn and a new office action was mailed on April 21, 2006.

3. STATUS OF CLAIMS

Claims 1-21 are pending in the present application. Claims 22-34 have been withdrawn from consideration due to a restriction/election requirement. Claims 1-21 have been rejected under 35 U.S.C. § 103(a) based on Togawa, U.S. Patent No. 6,240,530 (hereinafter, "Togawa"), and further in view of Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake").

Appellants appeal the rejections of claims 1-21.

4. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection.

5. SUMMARY OF INVENTION

As stated in the background section of the patent application, software has been developed to observe or monitor computer users. These software programs provide a wide variety of monitoring features. For example, some of these programs are able to log keystrokes of a user, log menu commands, take screen shots of a user's computer screen at various times, track use of various programs, track what web sites have been visited, monitor e-mail communications, etc. With the technology available today, most, if not all, of a computer user's activities on a computer can be observed and recorded. See the Appellants' patent application (hereinafter referred to as the "Specification"), page 2, lines 24-31; page 3, lines 1-13.

With the computer technology of today and with the observing programs now available and for those programs that will surely be developed and used in the future, computer users may be watched by third parties more often than many think. It would be highly beneficial to computer users if they could find out whether they are being observed by computer software and technology

and to know information about the observing activity and/or program. Specification, page 2, lines 24-31; page 3, lines 1-13.

As required by 37 C.F.R. § 41.37(c)(1)(v), a summary of claimed subject matter immediately follows. The references to the specification refer only to embodiments of the invention. The invention is defined by the claims. Accordingly, these references to the specification are not meant to limit the scope of the claims of the present invention in any way but are only provided because they are mandated by 37 C.F.R. § 41.37(c)(1)(v). All references are to the patent specification.

1. A computer program embodied in a computer-readable medium for scanning a computer for observer programs, the computer program comprising:

observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data; (pg. 7, lines 20-22; pg. 8, lines 9-20; pg. 11, lines 8-31; pg. 12, lines 1-31; pg. 13, lines 1-12; Figure 2, elements 34-48; pg. 14, lines 19-31; pg. 15, lines 1-31; pg. 16, lines 1-25)

reading instructions that read memory of the computer to obtain memory data; (pg. 7, lines 22-24; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 9, lines 5-14; pg. 13, lines 13-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer; (pg. 7, lines 24-26; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 13, lines 28-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; and (pg.

7, lines 26-29; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

outputting instructions that provide the results through a graphical user interface. (pg. 8, lines 6-8; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

21. A method embodied in a computer-readable medium for scanning a computer for observer programs, the method comprising:

using observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data; (pg. 7, lines 20-22; pg. 8, lines 9-20; pg. 11, lines 8-31; pg. 12, lines 1-31; pg. 13, lines 1-12; Figure 2, elements 34-48; pg. 14, lines 19-31; pg. 15, lines 1-31; pg. 16, lines 1-25)

reading memory of the computer to obtain memory data; (pg. 7, lines 22-24; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 9, lines 5-14; pg. 13, lines 13-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

comparing the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer; (pg. 7, lines 24-26; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 13, lines 28-31; pg. 14, lines 1-31; pg. 15, lines 1-31; pg. 16, lines 1-25; Figure 3, elements 50-60; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

generating results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; and (pg. 7, lines 26-29; pg. 7, lines 29-31; pg. 8, lines 1-5; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4;

pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

outputting the results through a graphical user interface. (pg. 8, lines 6-8; pg. 8, lines 21-31; pg. 9, lines 1-4; pg. 16, lines 26-31; Figure 4; pg. 17, lines 17-31; pg. 18, lines 1-31; pg. 19, lines 1-31; pg. 20, lines 1-31; pg. 21, lines 1-3; Figure 5; Figure 6)

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following issues are presented for review:

- A. Whether claims 1-21 are unpatentable under 35 U.S.C. § 103(a) based on Togawa in view of Drake.
- B. Whether a "Prior Art" legend must be added to Figure 1.

7. ARGUMENT

A. Claims 1-21 Rejected Under 35 U.S.C. § 103(a)

The Examiner rejected claims 1-21 under 35 U.S.C. § 103(a) based on Togawa, U.S. Patent No. 6,240,530 (hereinafter, "Togawa"), and further in view of Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake"). This rejection is respectfully traversed.

The M.P.E.P. states that

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.

The initial burden is on the examiner to provide some suggestion of the desirability of doing what the inventor has done. To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references.

M.P.E.P. § 2142.

Appellants respectfully submit that the claims at issue are patentably distinct from Togawa in view of Drake. Neither Togawa nor Drake teach or suggest all of the limitations in the claims.

Claim 1 recites “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.” Within this first claim limitation there are a number of claim limitations including (1) “observer data”, (2) “observer data comprising a plurality of observer program characteristics”, (3) “observer program characteristics descriptive of a plurality of observer programs”, and (4) “where the observer programs are programmed to observe activities on a computer system and to create log data.” Togawa does not teach or suggest any of these claim limitations. The Office Action has cited portions of Togawa and Drake as teaching or suggesting these claim elements. Each of these portions cited will be addressed in turn.

The Office Action cited Togawa, Figure 1, s1 in relation to this claim limitation. Figure 1 of Togawa is a flow diagram and s1 is a “virus detection and identification step.” Togawa, Figure 1. This does not teach or suggest “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.”

The Office Action also cited Col. 5, lines 10-19 of Togawa in relation to this claim limitation. The portion of Togawa states the following:

According to a further aspect of the present invention, there is provided an information processing apparatus which includes a memory for storing programs and data for information processing and a processing section for executing the programs to perform various information processing, comprising a virus detection and identification section for detecting a computer virus which infects the information processing apparatus and identifying a type of the detected computer virus, a virus type information registration section for registering information regarding the type of the detected computer virus identified by the virus detection and identification section into a storage area which is access-disabled in an ordinary operation of the information processing apparatus . . .

Togawa, Col. 5, lines 7-19. This does not teach or suggest “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.” All of the claim limitations must be considered. This portion of Togawa teaches virus detection. However, it does not teach or suggest “observer data”, nor does it teach or suggest “observer data comprising a plurality of observer program characteristics”, nor does it teach or suggest “observer program characteristics descriptive of a plurality of observer programs”, etc. Each of the claim limitations must be taught or suggested in the prior art references. None of these following limitations are taught or suggested in Togawa: “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.”

Togawa does not teach or suggest anything with respect to observer programs. The Office Action admitted this in stating that “Togawa fails to teach explicitly searching for observer programs.” Office Action, Page 3.

The Office Action also cited Drake, Figures 4, 5 and Col. 3, lines 31-52, in relation to this claim limitation. The portion in Col. 3 of Drake states the following:

This invention seeks to provide computer software having enhanced security features, to a process which substantially enhances the security of computer software (hereafter referred to as the improved process) and to a method by which to apply said improved process (hereafter referred to as the applicator).

The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

Preferably, the improved process also consists of including computer code to prevent decompilation, reverse-engineering, and disassembly by the inclusion of obfuscating code inserts, and the use of executable encryption.

Preferably, the improved process also consists of including code to prevent execution-tracing and debugging by the use of code designed to detect and prevent these operations.

Drake, Col. 3, lines 31-52.

This portion of Drake does not teach or suggest “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.” It does mention “rogue software eavesdropping” (Col. 3, lines 41-42) and “anti-spy techniques” (Col. 3, lines 43), but the mere mention of generic terms does not teach or suggest these claim elements. Figure 4 of Drake illustrates the known operation of a rogue eavesdropping program. Drake, Col. 4, lines 13-14. Figure 5 of Drake illustrates the interaction of the components of the updated application. Drake, Col. 4, lines 15-16. Claim 1 specifically requires “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.”

As shown, neither Togawa nor Drake teach or suggest all of the following claim limitations: “observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data.”

Claim 1 also recites “comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer.” Togawa does not teach or suggest this claim limitation. The Office Action has cited a portion of Togawa as teaching or suggesting this claim element. This portion of Togawa is as follows:

FIG. 1 illustrates in flow chart a virus extermination method according to an aspect of the present invention. Referring to FIG. 1, the virus extermination method illustrated includes a virus detection and identification step S1, a memory clearing step S3, an operating system fetching and starting up step S4 and a virus extermination step S5 in order to exterminate a computer virus as a software destroying factor which infects a computer system.

More particularly, in the virus detection and identification step S1, a computer virus as a software destroying factor which infects a computer system is detected and a type of the computer virus is identified. If such an infecting computer virus is detected in the virus detection and identification step S1 (the YES route of step S2), then information stored in all of those areas of a memory which are in a write-enabled state in an ordinary operation of the computer system is cleared in the memory clearing step S3.

Togawa, Col. 8, lines 14-30.

This portion of Togawa does not teach or suggest “comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer.” Col. 8, lines 14-30 of Togawa identifies “a virus detection and identification step S1,” Togawa states that if “such an infecting computer virus is detected in the virus detection and identification step S1 . . . , then information stored in all of those areas of a memory . . . is cleared in the memory clearing step S3.” Togawa, Col. 8, lines 25-30. This simply does not teach or suggest “comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer.” This claim limitation requires all of the elements therein including (1) “comparing instructions that compare the plurality of observer program characteristics with memory data characteristics”, (2) “to determine whether an observer program is present on the computer.”

Appellants do not agree with the Office Action’s characterization of Togawa as “teach[ing] a system for the detection and removal of computer malware.” Office Action, Page 3. The use of the term “malware” is much broader than what Togawa teaches. The term “malware” cannot be found anywhere in the Togawa reference using a standard text search. The title of Togawa is “Virus extermination method, information processing apparatus and computer-readable recording medium with virus extermination program recorded thereon.” Togawa only addresses virus detection and removal and, as a result, Appellants believe generalizing Togawa to “malware” is improper. Furthermore, the Office Action’s substitution of the word “malware” in place of virus detection suggests that the Office Action used improper hindsight reasoning in an attempt to broaden what Togawa teaches or suggests. Hindsight reasoning is, of course, improper.

As shown, neither Togawa nor Drake teach or suggest all of the limitations in claim 1. As a result, Appellants respectfully request that the rejection of claim 1 be withdrawn.

As set forth above, neither Togawa nor Drake teach or suggest all of the limitations in claim 1. Claims 2-20 depend directly or indirectly from claim 1. Thus, Appellants respectfully request that the rejection of claims 2-20 be withdrawn for at least the same reasons.

Claim 21 includes similar limitations as claim 1 which were argued above. Thus, Appellants respectfully request that the rejection of claim 21 be withdrawn for at least the same reasons.

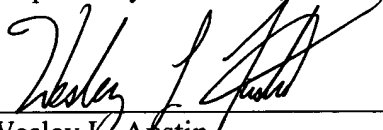
B. "Prior Art" Legend and Figure 1

The Office Action asked for a "Prior Art" legend to be added to Figure 1. Appellants respectfully request that the Examiner's objection be reversed for the following reasons.

Figure 1 is a "block diagram of the major hardware components of a computer used with the embodiments." Patent Application, Page 6, lines 8-9. The claims include elements that are illustrated in the exemplary embodiment in Figure 1. For example, claim 1 includes "memory of the computer to obtain memory data." The memory and the computer are both illustrated in one exemplary embodiment of Figure 1. Claim 23 also includes "a processor", which is illustrated in one exemplary embodiment shown in Figure 1. Thus, the exemplary embodiment shown in Figure 1 is illustrated and discussed in relation to Applicant's invention. Where elements of the claims are illustrated in Figure 1, Appellants do not think it is proper to require a "Prior Art" legend for Figure 1.

Appellants respectfully assert that claims 1-21 are patentably distinct from the cited references and that the rejection of claims 1-21 is improper. Reversal of the Examiner's rejections and allowance of the pending claims is respectfully requested.

Respectfully submitted,



Wesley L. Austin
Reg. No. 42,273
Attorney for Appellant(s)

Date: October 5, 2006

Wesley L. Austin, Esq.
Trapware Corporation
1244 E. 1650 S.
Bountiful, UT 84010
Telephone: (801) 296-0597

CLAIMS APPENDIX

Listing of Claims involved in the appeal (withdrawn claims are shown):

1. A computer program embodied in a computer-readable medium for scanning a computer for observer programs, the computer program comprising:
 - observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data;
 - reading instructions that read memory of the computer to obtain memory data;
 - comparing instructions that compare the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;
 - generating instructions that generate results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; and
 - outputting instructions that provide the results through a graphical user interface.
2. The computer program of claim 1 wherein the memory data includes startup commands.
3. The computer program of claim 1 wherein the memory data includes registry startup commands.
4. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer import table data and wherein the comparing instructions compare memory import table data from the memory data characteristics with the observer import table data to determine whether an observer program is present on the computer.

5. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer export table data and wherein the comparing instructions compare memory export table data from the memory data characteristics with the observer export table data to determine whether an observer program is present on the computer.
6. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer resource data and wherein the comparing instructions compare memory resource data from the memory data characteristics with the observer resource data to determine whether an observer program is present on the computer.
7. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer file content data and wherein the comparing instructions compare memory file content data from the memory data characteristics with the observer file content data to determine whether an observer program is present on the computer.
8. The computer program of claim 7 wherein the comparing instructions compare the observer file content data with the memory file content data at an offset address.
9. The computer program of claim 7 wherein the comparing instructions compare the observer file content data with a span of the memory file content identified by an offset address.
10. The computer program of claim 1 wherein the plurality of observer program characteristics includes observer module loading data and wherein the comparing instructions compare memory module loading data from the memory data characteristics with the observer module loading data to determine whether an observer program is present on the computer.
11. The computer program of claim 1 wherein the plurality of observer program characteristics includes OS observing functions and wherein the comparing instructions compare

memory functions from the memory data characteristics with the OS observing functions to determine whether an observer program is present on the computer.

12. The computer program of claim 1 wherein the memory data includes explorer extension data.
13. The computer program of claim 1 wherein the memory data includes file use information.
14. The computer program of claim 1 wherein the memory data includes process information.
15. The computer program of claim 1 wherein the memory data includes running process information.
16. The computer program of claim 1 wherein the memory data includes loaded modules information.
17. The computer program of claim 1 wherein the memory data includes driver data.
18. The computer program of claim 1 wherein the memory data includes kernel driver data.
19. The computer program of claim 1 wherein the computer program further comprises disabling instructions to disable the observer program if it is present on the computer, the disabling instructions implementing a method comprising:
entering a startup command to load a kill program before the observer program is started;
rebooting the computer;
starting the kill program by execution of the startup command; and
deleting an observer program startup command so that the observer program is not started.

20. The computer program of claim 19 wherein the method further comprises deleting observer program files.

21. A method embodied in a computer-readable medium for scanning a computer for observer programs, the method comprising:

using observer data comprising a plurality of observer program characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data;

reading memory of the computer to obtain memory data;

comparing the plurality of observer program characteristics with memory data characteristics to determine whether an observer program is present on the computer;

generating results from the comparing, wherein the results generated indicate whether the observer program is present on the computer; and

outputting the results through a graphical user interface.

22-34. (Withdrawn)

Appl. No. 10/027,714
Appeal Brief Dated June 20, 2005
Reply to Office Action of April 7, 2006

EVIDENCE APPENDIX

NONE.

Appl. No. 10/027,714
Appeal Brief Dated June 20, 2005
Reply to Office Action of April 7, 2006

RELATED PROCEEDINGS APPENDIX

NONE.